IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

DOUGLAS CASTELL, *individually and on behalf of all others similarly situated*,	)	
Plaintiff,	)	
v.	)	**Civil Case No. _____**
CHANGE HEALTHCARE INC., a Delaware corporation, UNITEDHEALTH GROUP INCORPORATED, a Delaware corporation, UNITEDHEALTHCARE, INC., a Delaware Corporation, and OPTUM, INC., a Delaware Corporation,	)	DEMAND FOR JURY TRIAL
Defendants.	)	

CLASS ACTION COMPLAINT

Table of Contents

CLASS ACTION COMPLAINT

Plaintiff, Douglas Castell, individually and on behalf of the Class defined herein of similarly situated persons ("Class Members"), alleges the following against Defendants Change Healthcare Inc. ("Change"), UnitedHealth Group Incorporated ("UnitedHealth"), UnitedHealthcare, Inc. ("UnitedHealthcare"), and Optum, Inc. ("Optum") (collectively, "Defendants") based upon personal knowledge with respect to himself and on information and belief as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendants' failure to secure the personal identifiable information ("PII")[1] and protected health information ("PHI")[2] (collectively "Private Information") of Plaintiff and the members of the proposed Classes and the accompanying failure to secure the systems and platforms necessary to timely and accurately process manufacturer savings card/"coupon" programs for otherwise very expensive (or unaffordable) prescription medications.

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, but not limited to, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Pursuant to the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations (collectively, "HIPAA"), "protected health information" includes all individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient.

2. Defendant Change—a unit of UnitedHealth's Optum subsidiary—is a "health technology giant" that provides revenue and payment cycle management services that lie at the heart of the U.S. healthcare system. Those services connect payers, providers, pharmacies, and patients. The services are critical to providing healthcare throughout the country.

3. Change is known to be the nation's largest commercial prescription processor, serving as a digital intermediary to verify a patient's insurance coverage for prescriptions, process "coupons" and "co-pay" cards provided by manufacturers to help patients (including uninsured or under-insured) afford expensive medications and treatments, and handling prescriptions and billing for more than 67,000 pharmacies across the U.S. healthcare system. The data flowing through the systems Change operates includes (at least) confidential patient health information, as well as banking information for providers.

4. According to Change, it processes 15 billion health care transactions annually—including a range of services that directly affect patient care, such as clinical decision support, eligibility verifications, and pharmacy operations—touches one out of every three U.S. patient records, and its "cloud-based network supports 14 billion clinical, financial, and operational transactions annually."

5. On February 21, 2024, UnitedHealth, the nation's largest insurer, filed a Form 8-K with the Securities and Exchange Commission disclosing that Change's systems had been infiltrated by a "suspected nation-state associated cyber security threat actor."

6. Subsequent reports identified the cybercriminals that accessed Change's system as the ransomware gang ALPHV/BlackCat, which claimed responsibility for the attack and claimed it has accessed and stolen confidential information, including health information, for millions of patients (the "Data Breach").

7. Reports indicate the attack was carried out as a ransomware attack in which ALPHV/BlackCat accessed multiple terabytes of sensitive health data to secure a large ransom payment, which it appears was made for about $22 million.

8. The Data Breach, against one of America's largest healthcare companies was described by the American Hospital Association as "the most serious incident of its kind leveled against a U.S. health care organization."

9. Aside from the many well-known harms associated with the theft and commoditization of healthcare-related data (e.g., illegal financial transactions using victim's Private Information), as the result of the Data Breach, pharmacies and providers were unable to process drug manufacturer coupons and "co-pay" cards, leaving uninsured or under-insured patients, such as Plaintiff, without those critical payment mechanisms they rely on to afford expensive medications and treatments.[3]

10. On or about February 28, 2024, cybercrime group "Blackcat" (also known as "ALPHV," referred to hereinafter as "ALPHV Blackcat") claimed credit on its darknet site for the attack, asserting that it stole from Change millions of sensitive records—over eight (six, by some accounts) terabytes of data—including medical insurance and health data on thousands of consumers, healthcare providers, pharmacies, and insurance providers. ALPHV Blackcat further acknowledged that its access and theft included data from Change partners, such as Medicare, Tricare, CVS Health, and other companies.

11. The attack was entirely foreseeable and avoidable. Indeed, in a Joint Cybersecurity Advisory issued on December 19, 2023, the Federal Bureau of Investigation ("FBI") and the

[3] *Who and what is the hack of UnitedHealth's tech unit affecting?*, Reuters (March 6, 2024) https://www.reuters.com/technology/cybersecurity/who-what-is-hack-unitedhealths-tech-unit-affecting-2024-03-06/ (last visited March 7, 2024).

Cybersecurity & Infrastructure Security Agency ("CISA") encouraged critical infrastructure organizations, such as Defendants, to implement their various recommendations as set forth in the advisory to reduce the likelihood and impact of inevitable ALPHV Blackcat ransomware and data extortion efforts. The FBI and CISA provided various step-by-step technical details associated with the ALPHV Blackcat criminal organization and its attack techniques, and advised organizations of "actions to take today," which included "prioritize remediation of known exploited vulnerabilities."[4]

12. Notwithstanding these publicized high-priority, emergent, and critical warnings, it is apparent from the reported nature and extent of the attack that Defendants failed to take reasonable, timely and appropriate measures to protect against the foreseeable, catastrophic cyberattack, including remediation ("patching") the known vulnerabilities.

13. As a direct and proximate result of Defendants' failures, Plaintiff and the Class Members have suffered and will indefinitely suffer serious injury.

14. Accordingly, Plaintiff, on behalf of himself and the estimated millions of similarly situated victims of the Data Breach, seeks to hold Defendants responsible for the injuries suffered as the result of their misconduct and failure to act, and demands appropriate monetary, equitable, injunctive, and declaratory relief.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 putative

[4] *See* FBI and CISA Joint Cybersecurity Advisory (December 19, 2023), available at: joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf (aha.org).

members in the proposed class, and at least one Class Member (e.g., Plaintiff) is a citizen of a state different from any Defendant.

16. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged are part of the same case or controversy.

17. This Court has personal jurisdiction over Defendants. Defendant Change is headquartered and routinely conducts business in the State where this District is located. Each of the Defendants have sufficient minimum contacts in this State, have intentionally availed themselves of this jurisdiction by conducting business in this State, including through marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

18. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District and Defendant Change is headquartered and does business in this Judicial District.

PARTIES

Plaintiff, Douglas Castell

19. Plaintiff Douglas Castell ("Plaintiff") is a citizen and resident of Levy County, Florida.

20. Plaintiff requires confidential prescription medication to treat a chronic condition.

21. Plaintiff participates in a manufacturer savings program "powered by Change Healthcare," which enables him to fill his necessary prescription medication at a lower, out-of-pocket cost per month, as opposed to the full out-of-pocket cost in excess of $1,000 per month he would have to pay without the manufacturer program.

22. Such savings programs are sometimes referred to as "coupons" or "savings cards."

23. On information and belief, Change undertook to carry out necessary parts of the processing, tracking, and payments in the manufacturer savings program that Plaintiff depends on and similarly undertook such services with respect to other similar prescription drug savings programs, savings cards programs, "coupons," and co-pay coverage programs.

24. For purposes of participating in the savings program, Plaintiff was required to provide his Private Information to his healthcare providers, including his pharmacy and, in turn, to Change (for purposes, at least, of processing his savings card transactions).

25. Plaintiff received no warnings from Defendants that they did not adequately secure and protect his Private Information or their savings card processing platform. Plaintiff learned of the Data Breach only after it had occurred, namely when his pharmacy informed Plaintiff that it could not fill his medication using the coupon due to the Data Breach. Defendants, however, have not informed Plaintiff of the Data Breach.

26. As the result of the Data Breach and Defendants' actions/inactions since, Plaintiff's coupon for his otherwise unaffordable and necessary medication could not be processed from at least February 21, 2024 to March 22, 2024. The pharmacy that handles Plaintiff's prescription and savings card transactions, like huge numbers of pharmacies across the country, could not process Plaintiff's coupon.

27. As a result, Plaintiff's ability to fill his necessary prescription medication was delayed and disrupted, depriving him of necessary medication for weeks and subjecting him to severe stress, anxiety, and emotional distress as he was exposed to severe personal and health risks, including suicidal ideation. As a result of the interruption of his medication, Plaintiff is now required to alter his dosage to "ramp up" to the dosage he was prescribed and taking prior to the disruption of his medication.

28. In addition, although Defendants have unreasonably failed to provide information concerning their own knowledge and understanding of the nature and scope of the Data Breach, Plaintiff reasonably believes based on public reports—and the severity and length of the disruption the Data Breach has and continues to cause to the U.S. healthcare system—that Defendants did not and are not maintaining his Private Information with adequate care and protection and that his Private Information was part of the massive volume of healthcare information exposed to the attack, which has been credibly reported to include ALPHV/BlackCat having accessed and held multiple terabytes of data for ransom.

29. Reasonable concern that his sensitive Private Information has been compromised, exposed, and subjected to exploitation has caused Plaintiff additional stress, anxiety, and distress. Since Plaintiff learned of the Data Breach, Plaintiff has spent, and will indefinitely continue to spend, considerable time monitoring for adverse personal impacts caused by unauthorized exposure of his Private Information, such as evidence of identity theft and the modification to or theft from his various financial accounts, and investigating the Data Breach for indications that his Private Information has been exploited and to what extent.

30. But for the Data Breach, Plaintiff would not have expended his time in this fashion.

31. In light of the amount and nature of the Private Information that ALPHV Blackcat claims to have authorized and/or stolen from Defendants—over eight terabytes of medical insurance and health data on thousands of healthcare providers, pharmacies, and insurance providers—Plaintiff has been and will remain at heightened risk for extortion, harassment, "spamming" and "phishing" attacks, identity theft, illegal financial transactions under his name, misuse or modification of his accounts, unauthorized purchases or money laundering, unauthorized loans or lines of credit, credit downgrade, and filing of false unemployment or similar claims.

Defendant, Change Healthcare Inc.

32. Change is a Delaware corporation, with principal executive offices located at 424 Church Street #1400, Nashville, Tennessee.

33. Change is a subsidiary of Optum, a subsidiary of UnitedHealth, and markets itself as "Part of Optum."

34. According to Form 10-K filed by UnitedHealth with the Securities Exchange Commission on or about February 24, 2023:

> On October 3, 2022, the Company acquired all of the outstanding common shares of [Change] and funded Change's payoff of its outstanding debt and credit facility for a total of $13.9 billion in cash. The combination of the Company and Change will connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients. Change brings key technologies, connections and advanced clinical decision, administrative and financial support capabilities, enabling better workflow and transactional connectivity across the health care system.

35. As part of the UnitedHealth healthcare empire, Change provides revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system.

Defendants, UnitedHealth, UnitedHealthcare, and Optum

36. UnitedHealth is a Delaware corporation, with principal executive offices located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, Minnesota.

37. UnitedHealthcare is a Delaware corporation with principal executive offices located at UnitedHealth Group Center, 9900 Bren Road East, Minnetonka, Minnesota.

38. Optum is a Delaware corporation with principal executive offices located at 13625 Technology Drive, Eden Prairie, Minnesota.

39. UnitedHealth is the parent corporation to UnitedHealthcare, Optum, and Change. Upon information and belief, UnitedHealth operates through four segments, which include UnitedHealthcare and three segments of Optum (i.e., Optum Health, Optum Insight, and OptumRx).

40. Optum has been a subsidiary of UnitedHealth since 2011, and is a parent corporation to Change, having acquired Change in or about October of 2022.

41. In its Form 10-K filed on or about February 24, 2023, UnitedHealth provided the following general overview of its and Optum's services:

> UnitedHealth Group Incorporated is a health care and well-being company with a mission to help people live healthier lives and help make the health system work better for everyone. Our two distinct, yet complementary business platforms—Optum and UnitedHealthcare—are working to help build a modern, high-performing health system through improved access, affordability, outcomes and experiences for the individuals and organizations we are privileged to serve.
>
> The ability to analyze complex data and apply deep health care expertise and insights allows us to serve people, care providers, businesses, communities and governments with more innovative products and complete, end-to-end offerings for many of the biggest challenges facing health care today.
>
> Optum combines clinical expertise, technology and data to empower people, partners and providers with the guidance and tools they need to achieve better health. Optum serves the broad health care marketplace, including payers, care providers, employers, governments, life sciences companies and consumers, through its Optum Health, Optum Insight and Optum Rx businesses. These businesses improve overall health system performance by optimizing care quality and delivery, reducing costs and improving consumer and provider experience, leveraging distinctive capabilities in data and analytics, pharmacy care services, health care operations, population health and health care delivery.
>
> UnitedHealthcare offers a full range of health benefits, enabling affordable coverage, simplifying the health care experience and delivering access to high-quality care. UnitedHealthcare Employer

> & Individual serves employers ranging from sole proprietorships to large, multi-site and national employers, public sector employers and individual consumers. UnitedHealthcare Medicare & Retirement delivers health and well-being benefits for Medicare beneficiaries and retirees. UnitedHealthcare Community & State manages health care benefit programs on behalf of state Medicaid and community programs and their participants.

42. UnitedHealth is regarded as the largest insurer in the United States and, based upon its revenue, the largest company in the U.S. healthcare sector. UnitedHealth maintains several offices within Tennessee including, upon information and belief, offices in Maryville, Kingston, Murfreesboro, and Cordova, Tennessee.

43. UnitedHealthcare markets and sells insurance-related products and services directly to Tennessee consumers, including health insurance coverage plans, short term health insurance plans, individual and family Affordable Care Act marketplace plans, and supplemental, dental, and vision insurance plans within Tennessee. By way of example, on its website,[5] UnitedHealthcare states, in pertinent part:

> Tennessee health insurance plans
>
> You have more insurance options for your health than you think, Tennessee.
>
> If you're self-employed or without insurance from your employer—in other words, you're looking for individual or family health insurance in Tennessee—you might be looking for Affordable Care Act insurance. However, we want to make you aware of the whole range of individual and family insurance products we have available in your state.

44. UnitedHealthcare states further on its website,[6] in pertinent part:

> See why Tennesseans choose UnitedHealthcare.

[5] https://www.uhc.com/individuals-families/tennessee.

[6] https://www.uhc.com/communityplan/tennessee.

> Whatever plan you choose, UnitedHealthcare will help you get the care you need.
>
> - Large variety of network providers
> - Low- or no-cost prescription drugs
> - Well visits, routine shots
> - Dental and vision services
> - Transportation to medical appointments.

45. Optum—via Optum Health, Optum Insight, and Optum Rx—markets and sells insurance-related products and services to Tennessee consumers, including through partnership with TennCare Medicaid plans for pharmacy and other needs, through UnitedHealthcare's Community Plan, and through benefits maintained for state and higher education employees and local education and government members of the State of Tennessee.[7]

REGULATORY FRAMEWORK AND STANDARDS GOVERNING CREATION, COLLECTION, MAINTENANCE, AND USE OF PRIVATE INFORMATION

46. Federal and state regulators have established security standards and issued guidelines and recommendations to reduce the risk of cyberattacks, data breaches, and the resulting harm to consumers and the healthcare industry. There are a number of state and federal laws, requirements, and industry standards governing the creation, collection, protecting, and use of Private Information.

47. Defendants were or should have been fully aware of the obligations, guidelines, and recommendations with respect to their creation, collection, maintenance, protection, and use of Private Information.

A. The Health Insurance Portability and Accountability Act (HIPAA)

[7] *See, e.g.*, https://www.optumrx.com/oe_tenncare/landing (last visited March 7, 2024) and https://www.tn.gov/partnersforhealth/other-benefits/emotional-wellbeing-solutions.html (last visited March 7, 2024).

48. Change states in its Global Privacy Notice that it "functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers as its primary business function, so Change Healthcare's creation, collection, use, and disclosure of protected health information is guided by HIPAA and the terms of a business associate agreement and other contracts."[8]

49. As a business associate covered under HIPAA (45 C.F.R. § 160.102), Defendants are required to comply with HIPAA Rules, including the Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("*Standards for Privacy of Individually Identifiable Health Information*"), and the Security Rule ("*Security Standards for the Protection of Electronic Protected Health Information*"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.[9]

50. These rules establish national standards for the protection of patient information, including Private Information, defined under the standards as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

---

[8] Change Healthcare Global Privacy Notice, Effective December 2023, available at: https://www.changehealthcare.com/privacynotice?adobe_mc=mcorgid%3d26cd3a665c7d19990a495d73%2540adobeorg%7cts%3d1709006189&adobe_mc=MCORGID%3D26CD3A665C7D19990A495D73%2540AdobeOrg%7CTS%3D1709006561 (last visited February 26, 2024).

[9] HIPAA's *Standards for Privacy of Individually Identifiable Health Information* (also known as the "Privacy Rule") establishes national standards for the protection of medical records and other personal health information. HIPAA's *Security Standards for the Protection of Electronic Protected Health Information* (also known as the "Security Rule") establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. Per the U.S. Department of Health and Human Services' website, "[t]he Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." *See* https://www.hhs.gov/hipaa/for-professionals/security/index.html.

51. Title II of HIPAA contains what are known as the Administrative Simplification provisions.[10] These provisions require, among other things, that the U.S. Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification of HIPAA. These regulations include 45 C.F.R § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

52. Among numerous obligations imposed by HIPAA, Defendants are required to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information."[11] "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media."[12]

53. HIPAA requires covered entities and business associates of covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information. Covered entities and business associates must also implement safeguards to ensure the confidentiality, integrity, and availability of such information. Safeguards must include physical, technical, and administrative components.

54. The Security Rule requires covered entities, including business associates, to the do the following:

[10] *See* 42 U.S.C. §§ 1301, *et seq.*

[11] *See* 45 C.F.R. § 164.302.

[12] *See* 45 C.F.R. § 164.103.

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

55. HIPAA also requires Defendants to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights."[13]

56. Because most healthcare providers and health plans do not carry out all of their healthcare activities and functions by themselves, and often use the services of a variety of other persons or businesses, the Privacy Rule allows a covered provider and health plan to disclose protected health information to "business associates"[14] if the provider or plan obtains satisfactory

[13] 45 C.F.R. § 164.312(a)(1).

[14] A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity. Common functions and activities of business associates include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Common business

assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

57. Defendants are also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[15] Both HIPAA and HITECH obligate Defendants to follow reasonable security standards, respond to, contain, and mitigate security violations, and protect against disclosure of Private Information.[16]

58. In addition, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

B. The Federal Trade Commission Act (FTCA)

59. The Federal Trade Commission ("FTC") "works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers." The Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair or deceptive acts or practices in or affecting commerce."

---

associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

[15] *See, e.g.*, 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

[16] *See, e.g.*, 45 C.F.R § 164.306(a)(1) and § 164.306(a)(3)l; 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

60. The FTC has determined that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA. The FTC states on its website:[17]

> This means that companies must not mislead consumers about—among other things—what's happening with their health information. It also means you must ensure your health data practices aren't causing more harm than good. The FTC Act's obligations apply to HIPAA-covered entities and business associates, as well as to companies that collect, use, or share health information that aren't required to comply with HIPAA.

61. Consequently, the FTC has issued numerous guidelines to identify best data security practices that business, such as Defendants, should employ to protect against unlawful exposure of Private Information.

62. The FTC's guidance for businesses underscores the importance of implementing and maintain reasonable data security practices.[18] For example, the FTC offers the following general guidelines:

- In managing confidential information, businesses should factor security into the decision making in every department of the business—personnel, sales, accounting, information technology, etc.
- Don't collect personal information you don't need, and hold on to information only as long as you have a legitimate business need.
- Don't use personal information when it's not necessary.

---

[17] *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach (last visited February 26, 2024).

[18] *Start with Security: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/start-security-guide-business#start (last visited February 26, 2024).

- Use an intrusion detection system to expose a breach as soon as it occurs.
- Watch for large amounts of data being transmitted from the system.
- Have a response plan in the event of a breach.

63. With respect to updates and patches to third-party software, the FTC states that outdated software undermines security, the solution being to update software regularly, implement third-party patches as they are issued, prioritize patches by the severity of the threat they are designed to avert, and use automated tools to track which version of software is running and whether updates are available.

64. Consequently, the FTC strongly encourages businesses to "[p]ut procedures in place to keep your security current and address vulnerabilities that may arise," including to "[c]heck expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems."[19] The FTC's website cites an example case, wherein it charged that a business failed to patch a critical vulnerability because its patch management policies and procedures were inadequate.

65. With respect to security warnings in regard to vulnerabilities, the FTC cautions businesses to heed credible security warnings and move quickly to fix them. The FTC also strongly encourages businesses to "[h]ave an effective process in place to receive and address security vulnerability reports." Citing an example case, wherein the FTC charged that a business' alleged delay in responding to warnings meant that the vulnerabilities found their way onto additional

[19] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited February 26, 2024).

devices and across multiple system versions, the FTC warns: "When vulnerabilities come to your attention, listen carefully and then get a move on."

66. The FTC has brought and routinely brings enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice prohibited by the FTCA. Orders derived from these enforcement actions explicate the measures businesses are required to take to satisfy obligations with respect to data security.

C. State Laws Concerning Private Information

67. At least 24 states have enacted laws addressing data security practices, requiring businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

D. Industry Standards

68. Cybersecurity experts consistently recognize the healthcare industry as particularly vulnerable to cyberattacks, primarily due to the valuable nature of the Private Information derived through healthcare-related services and products.

69. Various cybersecurity industry best practices have been published, are readily available, and should be consulted as a go-to source for an entity instituting, developing, maintaining, or enhancing its cybersecurity standards.

70. These practices include, across all industries encountering Private Information, education and appropriate access restriction for all personnel in regard to proper creation, collection, maintenance, and use of Protected Information; enforcing strong password and similar protections, including multi-factor authentication; applying multi-layer security measures

(including firewalls, anti-virus, and anti-malware software); monitoring for suspicious or irregular traffic to servers, credentials used to access servers, activity by known or unknown users, and server requests; implementing encryption[20] to render data unreadable without proper authorization; and regular back up of data.

71. Additional cybersecurity best practices are especially prevalent within the healthcare industry, including, but not limited to, installing appropriate malware detection software, monitoring and limiting network posts, securing web browsers and e-mail systems, configuring network infrastructure (like firewalls, switches, and routers), safeguarding physical security systems, training staff on key cybersecurity aspects, monitoring for vulnerability alerts, and promptly detecting and addressing vulnerability alerts prior to exploitation by cybercriminals.

72. In addition to commonly recognized industry best practices, the National Institute of Standards and Technology ("NIST") and the Center for Internet Security, Inc. ("CIS")[21] have established standards for reasonable cybersecurity readiness.

---

[20] HHS defined "encryption" as a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plan, comprehensible text. *See* https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html (last visited February 26, 2024).

[21] CIS is a community-driven nonprofit responsible for globally recognized best practices for securing IT systems and data, including a prescriptive, prioritized, and simplified set of best practices in cybersecurity (referred to as "CIS Controls") and consensus-based prescriptive configuration recommendations of global cybersecurity experts (referred to as "CIS Benchmarks"). Per the CI website, the CIS Controls are a general set of recommended practices for securing a wide range of systems and devices, whereas CIS Benchmarks are guidelines for hardening specific operating systems, middleware, software applications, and network devices. The need for secure configurations is referenced throughout the CIS Controls. In fact, CIS Control 4 specifically recommends secure configurations for hardware and software on mobile devices, laptops, workstations, and servers. Both the CIS Controls and the CIS Benchmarks are developed by communities of experts using a consensus-based approach. *See* https://www.cisecurity.org/controls/cis-controls-faq (last visited February 27, 2024).

73. Recognizing that the national and economic security of the United States is dependent upon the reliable function of critical infrastructure, President Barrack Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February of 2013. Executive Order 13636 directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. Created through collaboration between industry and government, the voluntary framework promotes the protection of critical infrastructure, and provides standards, guidelines, tools, and technologies to protect health information technology systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services.

74. For example, NISTIR 8374, a NIST publication titled "Ransomware Risk Management: A Cybersecurity Framework Profile," provides the following basic ransomware tips:

- Educate employees on avoiding ransomware infections.
    - Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.
    - Avoid using personal websites and personal apps—like e-mail, chat, and social media—from work computers.
    - Don't connect personally owned devices to work networks without prior authorization.
- Avoid having vulnerabilities in systems that ransomware could exploit.
    - Keep relevant systems fully patched. Run scheduled checks to identify available patches to install these as soon as feasible.

- Employ zero trust principles in all networked systems. Manage access to all network functions and segment internal networks where practical to prevent malware from proliferating among potential target systems.
- Allow installation and execution of authorized apps only. Configure operating systems and/or third-party software to run only authorized applications.
- Inform your technology vendors of your expectations (e.g., in contract language) that they will apply measures that discourage ransomware attacks.

- Quickly detect and stop ransomware attacks and infections.
  - Use malware detection software such as antivirus software at all times. Set it to automatically scan emails and flash drives.
  - Continuously monitor directory services (and other primary user stores) for indicators of compromise or active attack.
  - Block access to untrusted web resources. Use products or services that block access to server names, IP addresses, or ports and protocols that are known to be malicious or suspected to be indicators of malicious system activity.
- Make it harder for ransomware to spread.
  - Use standard user accounts with multi-factor authentication versus accounts with administrative privileges whenever possible.
  - Introduce authentication delays or configure automatic account lockout as a defense against automated attempts to guess passwords.

- Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has only the necessary access following the principle of least privilege.
- Store data in an immutable format (so that the database does not automatically overwrite older data when new data is made available).
- Allow external access to internal network resources via secure virtual private network (VPN) connections only.

- Make it easier to recover stored information from a future ransomware event.
  - Make an incident recovery plan. Develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization and business continuity plans for those critical services.
  - Back up data, secure backups, and test restoration. Carefully plan, implement, and test a data backup and restoration strategy—and secure and isolate backups of important data.
  - Keep your contacts. Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement, legal counsel, and incident response resources.

FACTUAL ALLEGATIONS

A. Change's Business

75. Change is a "health technology giant" which provides revenue and payment cycle management that connects payers, providers, and patients within the U.S. healthcare system.

76. Change is regarded as the nation's largest commercial prescription processor, working with thousands of insurance companies, doctors, pharmacists, and hospitals to help determine patient responsibility for payment. Change handles prescriptions and billing for more than 67,000 pharmacies across the U.S. healthcare system.

77. According to Change, it processes 15 billion health care transactions annually—including a range of services that directly affect patient care, such as clinical decision support, eligibility verifications and pharmacy operations—touches one in every three U.S. patient records,[22] and its "cloud-based network supports 14 billion clinical, financial, and operational transactions annually."[23]

78. Change also states on its website:[24]

> The Change Healthcare Platform provides industry-leading analytics, expansive data, and unparalleled connection and data transfer between providers, payers, and consumers to help improve workflows, increase administrative and financial efficiencies, and improve clinical decisions.

79. Change further states on its website:

> We champion innovation through our unified platform to enable a better coordinated, more efficient, and increasingly collaborative healthcare system—one that enables operational efficiencies,

[22] AHA Letter to HHS on Implications of Change Healthcare Cyberattack, available at: https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack (last visited February 28, 2024); Sead Fadilpasic, *Change Healthcare hit by major cyberattack—US health tech giant sees website taken offline, login pages unavailable*, https://www.msn.com/en-us/news/technology/change-healthcare-hit-by-major-cyberattack-us-health-tech-giant-sees-website-taken-offline-login-pages-unavailable/ar-BB1iIJwV (last visited February 28, 2024).

[23] https://www.changehealthcare.com/platform (last visited February 29, 2024).

[24] https://www.changehealthcare.com/about (last visited February 26, 2024).

> optimizes financial performance, and enhances the healthcare experience.

80. With respect to Private Information, Change states on its website[25] that it uses "Leading-Edge Technology" to secure customer payment information and accounts. According to Change, it "leverage[s] the latest technology, public and private data sources to fortify our processes and ensure your information is protected."

81. The Change Healthcare Global Privacy Notice ("Global Privacy Notice") states in pertinent part:

> Privacy matters to Change Healthcare, so we follow a privacy framework that helps us to manage and protect your personal information in the products and services we provide ("Services") and on our websites ("Sites"). This Global Privacy Notice ("Global Notice") describes how Change Healthcare collects uses, and shares the personal information from our Sites and Services, the rights and choices that you have about your personal information, and how you can contact us about our privacy practices. Whether you are new to Change Healthcare or a long-time user, please take a moment to review our practices, and if you have any questions contact us through the information in the **How to Contact Us** section below. [emphasis in original]

82. The Global Privacy Notice includes a section titled "Information We Collect From You," which states, in pertinent part:

> Change Healthcare collects personal information directly from you, automatically from your devices when you interact directly with our Sites and Services, and from other sources described in the Supplemental Notices. When you interact directly with our Sites and Services, you may not be required to provide us with certain data requested; however, some data is necessary for the purposes described in this Global Notice and if you fail to provide any required data, you may not be able to access our Sites and Services. Where possible, we will allow you to interact with us anonymously or using a pseudonym. However, for most of our functions and activities we usually need your name and contact information.

[25] https://support.changehealthcare.com/fraud-prevention (last visited February 26, 2024.

- **Identifiers:**
    - We collect your name, phone number, email address, mailing address, and contact address when you create an account or contact us via the Site and the Services. If you choose to create an account, you will also be asked to create a username and password, and we will assign one or more unique identifiers to your profile. We use this information to provide our Services, respond to your requests, and send information and advertisements to you.

    - We collect a unique numerical identifier, assigned to you by a Cookie, automatically when you use the Site and Services in order to identify you, provide our Services, keep you logged in to our Sites, prevent fraud, and provide you with targeted information and offers.

- **Payment information:** We, or a service provider working on our behalf, collect your payment information when you provide it in order to complete a transaction. This information includes your credit card number or bank account number. We use this information to facilitate payments and transactions.

- **Commercial information:** When you engage in transactions with us, we create records of transactions. We may use this information to measure the effectiveness of our Sites and Services and to provide you with targeted information, advertisements, and offers.

- **Visual information:** We may collect visual information such as profile pictures associated with any account you create if you choose to upload one.

- **Professional or employment-related information:** We collect your business contact information when you contact us regarding our Site and Services, or when you interact with us at trade shows. We may also collect your business contact information in the course of providing the Services. We otherwise do not collect your professional or employment-related information.

- **Inferences drawn to create a profile about a consumer reflecting the consumer's preferences or characteristics:** We analyze your actual or likely preferences through a series

> of computer processes and add our observations to your internal profile. We use this information to gauge and develop our marketing activities, to measure the appeal and effectiveness of our Sites and Services, applications, and tools, and to provide you with targeted information, advertisements, and offers.
>
> - **Browser and device data:** We may collect your device type, operating system and version, IP address, general geographic location as indicated by your IP address, browser type, screen resolution, device manufacturer and model, language, plug-ins, add-ons and the language version of the Site you are visiting.
>
> - **Usage data:** We collect information about the time you spend on the Site, the content you view and features you access, the pages that led or referred you to our Site, language preferences, how you interact with available content, and entered search terms.
>
> - **Your [s]ite [a]ctivity:** We collect any information you choose to include in your messages or responses when interacting with us through our Sites and Services, including via online communities and forums, inquiry forms, our support portal, or our Chatbox messaging service and other messaging services, including any information you provide when you complete a survey administered by us or by a supplier acting on our behalf.
>
> - **Social media:** We collect information that you make available to us on social media platforms (such as by clicking on a social media icon linked from our Sites and Services), including your account ID or username and other information included in your posts. [emphasis in original]

83. The Global Privacy Notice includes a section titled "Information We Collect From Other Sources," which states, in pertinent part:

> We may obtain information about you from other sources such as data brokers, customers, credit reporting agencies, social networks, partners with which we offer co-branded services or engage in joint marketing activities, and publicly available sources such as data in the public domain.

> We also may receive information about you from outside suppliers through your online activities on websites and connected devices over time and across websites, devices, apps and other online features and services.
>
> These other sources help us update, expand, and analyze our records; identify new customers; determine you or your organization's advertising or purchasing preferences; or prevent or detect fraud. We combine such information with information we have collected about you through our Sites and Services. We will treat the combined information in accordance with this Privacy Notice.

84. In light of Change's representations as to its vast influence and involvement in the U.S. healthcare industry—i.e., 15 billion health care transactions annually and touches one out of every three U.S. patient records—and the corresponding amounts of sensitive data it creates, collects, maintains, and uses, Defendants were and continue to be particularly susceptible to cyberattack.

B. The Data Breach

85. On or about February 21, 2024, Change experienced a data breach event (i.e., the Data Breach) through which (on information and belief) Plaintiff's and Class Members' Private Information in possession of Change and/or Defendants was obtained by an unauthorized party. According to publicly available information, including statements by Defendants, Change's systems were accessed by cybercriminals.

86. According to publicly available information, the data breach event was a ransomware attack, wherein the cybercriminals accessed Change's systems and encrypted Change's (and, upon information and belief, multiple other entities') data to hold it hostage with the aim of securing a large ransom payment.

87. In a Form 8-K report filed with the Securities Exchange Commission on February 21, 2024, UnitedHealth stated:

Item 1.05. Material Cybersecurity Incidents.

On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.

During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at https://status.changehealthcare.com/incidents/hqpjz25fn3n7. Please access that site for further information.

As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations. [emphasis in original]

88. On or about February 28, 2024, notorious cybercrime group ALPHV Blackcat claimed on its darknet site responsibility for the attack, claiming it stole from Change millions of sensitive records—over eight terabytes of data—including medical insurance and health data on thousands of healthcare providers, pharmacies, and insurance providers.

89. One day later, on February 29, 2024, UnitedHealth confirmed the ransomware attack on its subsidiary, stating: "Change Healthcare can confirm we are experiencing a cyber

security issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat."[26]

90. Media sources indicate that, on March 1, 2024, Change paid to ALPHV Blackcat a ransom in response to the attack, in the amount of 350 bitcoins, or approximately $22 million. *See, e.g., Hacking gang behind pharmacy chaos shuts down again. Will it matter?* (March 6, 2024) https://www.washingtonpost.com/technology/2024/03/06/ransomware-gang-alphv-shuts-down/ (last visited March 6, 2024).

C. Change Data Breach Disrupted Services Nationwide

91. As the result of the Data Breach, healthcare organizations were paralyzed and scrambling as they were suddenly without access to Change's mission-critical services, such as claims processing for prescriptions and basic banking, payroll, etc. Processing of critical manufacturer coupons and co-pay cards likewise was disrupted, leaving uninsured and under-insured patients without affordable access to expensive medications and treatments.

92. Following the attack and continued to date, health systems throughout the United States—including hospitals, physician groups, dental clinics, and pharmacies—reported that they were unable to fulfill or process prescriptions through patients' insurance and/or manufacturer coupon/co-pay programs, making prescription medication inaccessible.[27]

---

[26] Media sources indicate that, on March 1, 2024, Change paid to ALPHV Blackcat a ransom in response to the attack, in the amount of 350 bitcoins, or approximately $22 million. *See, e.g., Hacking gang behind pharmacy chaos shuts down again. Will it matter?* (March 6, 2024) https://www.washingtonpost.com/technology/2024/03/06/ransomware-gang-alphv-shuts-down/ (last visited March 6, 2024).

[27] As explained by the operator of seven Kansas pharmacies, the system outage prevented insurance verification and, thus, impacted patient ability to obtain medication. While some patients may have been able to pay cash if the medication is relatively inexpensive, others were unable to obtain more costly treatments for flu or COVID-19. *A Cyberattack on UnitedHealth Unit Disrupts Prescription Drug Orders*, The New York Times (February 26, 2024), available at:

93. In response to the cyberattack, the American Hospital Association stated in a February 26, 2024 letter to HSS,[28] in pertinent part:

> This unprecedented attack against one of America's largest health care companies has already imposed significant consequences on hospitals and the communities they serve. Although the full scope of the impact is still unclear, Change Healthcare's vast nationwide reach suggests that it could be massive. According to Change Healthcare, the company processes 15 billion health care transactions annually and touches 1 in every 3 patient records. These transactions include a range of services that directly affect patient care, including clinical decision support, eligibility verifications and pharmacy operations. All of these have been disrupted over the past several days. Thankfully, Change Healthcare has informed our members that its prior authorization portals are active, but our members are reporting that a substantial portion of their claims still cannot be processed, nor can they complete eligibility checks necessary to determine whether a patient's insurance covers a prospective treatment.
>
> Change Healthcare's downed systems also will have an immediate adverse impact on hospitals' finances and the work they do every day to care for patients and communities. Their interrupted technology controls providers' ability to process claims for payment, patient billing and patient cost estimation services. Any prolonged disruption of Change Healthcare's systems will negatively impact many hospitals' ability to offer the full set of health care services to their communities. After all, without this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services. In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers.

---

https://www.nytimes.com/2024/02/26/health/cyberattack-prescriptions-united-healthcare.html (last visited February 29, 2024).

[28] AHA Letter to HHS on Implications of Change Healthcare Cyberattack, available at: https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack (last visited February 28, 2024).

> We appreciate that the resolution to this attack ultimately lies with Change Healthcare and its parent company UnitedHealth Group. We are in communication with their leadership and have asked for certain support, including greater transparency about the nature and scope of the attack, an anticipated timeline for resolution, and temporary access to advanced payments to help providers weather the period while normal claims processing functions are down.

94. The grave concerns raised by the American Hospital Association have materialized and continue to materialize.

95. A spokesman for UnitedHealth estimated that more than 63,000 pharmacies nationwide have been affected by the attack.[29]

96. Unfortunately for patients who required prescription medication following the cyberattack, they were forced to either forgo critical prescription medication or, if possible, pay out of pocket and without guarantees of reimbursement.

97. Most of the millions of impacted patients will not be aware that the Data Breach has affected their medical data and ability to obtain necessary prescription medication "until something goes wrong" when they try to fill a prescription or visit a provider.[30]

98. In addition to the impact on prescription medication, healthcare providers throughout the U.S. were locked out of processing payments and, in turn, were "struggling to get paid" following the ransomware outage, resulting in overdue payments, interest accumulation, and other financial harm.[31]

---

[29] *WA pharmacies, health systems reel from UnitedHealthcare cyberattack* (February 29, 2024), available at: https://www.seattletimes.com/seattle-news/health/wa-pharmacies-health-systems-reel-unitedhealthcare-cyberattack/ (last visited February 29, 2024).

[30] *How a health-care cyberattack may affect your prescription drug access*, https://www.washingtonpost.com/wellness/2024/03/05/change-healthcare-hack-prescriptions-affect/ (last visited March 6, 2024).

[31] According to the proprietor of a Michigan laboratory, over a week after the cyberattack, the lab remained "100 percent down when it comes to billing right now," while six small providers

99. In response to the Data Breach, the American Hospital Association, which represents more than 5,000 hospitals and healthcare providers, advised its members on February 22, 2024 to disconnect from "mission critical services" provided by Optum (using Change).

100. Following the Data Breach, Tricare, the U.S. military's health insurance provider for active military personnel, said in a statement that the ongoing cyberattack was "impacting all military pharmacies worldwide and some retail pharmacies nationally." As of February 28, 2024, Tricare's website stated:[32]

> Change Healthcare Cyberattack Impact on MHS Pharmacy Operations
>
> A reported cyberattack on the nation's largest commercial prescription processor, Change Healthcare, continues to affect military clinics and hospitals worldwide. On February 21, Change Healthcare disconnected their systems to protect patient information. This is impacting all military pharmacies worldwide and some retailers nationally.
>
> As of February 28, 2024, military clinics and hospitals will continue to provide prescriptions through manual procedures until this issue is resolved. Military pharmacies will give priority to urgent prescriptions followed by routine prescriptions. Each military hospital and clinic will continue to offer pharmacy operations based on their local manning and resources. Please be patient while pharmacies take longer than usual to safely fill prescription needs.
>
> It is unknown at this time when the issue will be resolved. Beneficiaries are encouraged to contact their military hospital and clinic or retail pharmacy for the latest local updates.

---

reported to Reuters that "they were unable to process claims and were racking up thousands of dollars in overdue payments." *Healthcare providers hit by frozen payments in ransomware outage*, Reuters (February 29, 2024), available at: https://www.msn.com/en-us/money/companies/healthcare-providers-hit-by-frozen-payments-in-ransomware-outage/ (last visited February 29, 2024).

[32] https://tricare.mil/GettingCare/VirtualHealth/SecurePatientPortal/PatientPortalOutages (last visited February 28, 2024).

101. Ransomware and cyberattacks can be particularly dangerous within the healthcare industry as they have also been proven to cause immediate harm to patients' physical safety in addition to lack of prescription or treatment accessibility. By way of examples, according to John Riggi, the national advisor for cybersecurity and risk at the American Hospital Association, "when systems go dark, diagnostic technologies like CT scanners can go offline and ambulances carrying patients are often diverted, which can delay lifesaving care."[33]

102. In addition, ransomware and cyberattacks, such as the instant Data Breach, have devastating effects on substance abuse and mental health patients and providers across the country. According to a joint statement released by the National Council for Mental Wellbeing and the National Association of Addiction Treatment Providers in response to the Data Breach, "[i]n the midst of an overdose crisis and an increased demand for mental health treatment, this disruption in vital services has left patients vulnerable to crisis, as behavioral health providers are unable to obtain insurance approval or payment for their services."[34]

D. Defendants Failed to Comply with Regulatory Requirements and Standards, and Breached Contracts with and Duties Owed to Plaintiff and Class Members

103. On information and belief, Defendants violated HIPAA and HITECH. By way of examples, on information and belief, Defendants failed to maintain adequate security practices, systems, and protocols to prevent data loss (e.g., Defendants failed to heed credible security warnings, maintain adequate patch management policies and procedures, detect alerts in regard to

[33] *Ransomware group Blackcat is behind cyberattack on UnitedHealth division, company says* (February 29, 2024), https://www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html (last visited February 29, 2024).

[34] *Large Scale Cyberattacks Disrupt Essential Substance Abuse and Mental Health Services*, National Association of Addiction Treatment Providers (March 7, 2024) https://www.naatp.org/resources/news/large-scale-cyberattacks-disrupt-essential-substance-use-and-mental-health-services (last visited March 7, 2024).

vulnerabilities affecting their systems, and to properly update and patch third-party software), failed to mitigate the risks of a data breach and loss of data, failed to ensure the confidentiality and protection of Private Information, failed to encrypt or otherwise adequately protect Plaintiff's and Class Members' Private Information, and failed promptly and meaningfully notify Plaintiff and Class Members about the Data Breach.

104. On information and belief, Defendants failed to comply with the FTCA. By way of examples, on information and belief, Defendants failed to heed credible security warnings; failed to maintain adequate patch management policies and procedures; failed to detect alerts in regard to vulnerabilities affecting its systems; failed to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failed to properly use automated tools to track which versions of software were running and whether updates were available; failed to implement appropriate procedures to keep security current and address vulnerabilities, including failure to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities; and failed to encrypt or otherwise adequately protect Plaintiff's and Class Members' Private Information.

105. On information and belief, Defendants' failure to protect and safeguard the Private Information of Plaintiff and Class Members resulted in the disclosure of such information to one or more third parties (ALPHAV) without consent, in violation of HIPAA and FTCA. Such disclosure was not necessary to carry out the purpose for which Defendants received the information, nor was it permitted by statute, regulation, or order.

106. Defendants' violations of HIPAA and FTCA, as set forth above, were reckless or, at the very least, negligent.

107. On information and belief, Defendants also failed to implement and comply with industry standards in regard to cybersecurity. By way of examples, Defendants failed to meet the minimum standards of any of the following best practices and frameworks: CIS and NIST publications (including, without limitation, "Ransomware Risk Management: A Cybersecurity Framework Profile"), the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and CIS's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness and response.

E. The Private Information Accessed in the Data Breach is Highly Valuable

108. The Private Information of consumers is a valuable commodity and, consequently, a frequent intentional target to cybercriminals.

109. The value of Private Information is axiomatic considering the value of "big data" in corporate America and that consequences of cybercrimes include heavy criminal penalties. The risk-to-reward analysis illustrates, beyond question, that Private Information has considerable market value.

110. Indeed, the U.S. Attorney General confirmed in 2020 that "hackers" target consumers' sensitive personal information because it "has economic value."[35]

111. Numerous sources cite "dark web" pricing for stolen Private Information.[36]

[35] *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (February 10, 2020), available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited February 27, 2024).

[36] In pertinent part, Wikipedia defines the "dark web" as:

112. According to one report, a healthcare data record may be valued at up to $250.00 per record on the black market, compared to $5.40 for the next highest value record (i.e., a payment card).[37]

113. According to various other sources, Private Information can be sold at prices ranging from $40.00 to $200.00 per record, bank details can be sold at prices ranging from $50.00 to $200.00 per record,[38] and a stolen credit or debit card number can sell for $5.00 to $110.00.[39]

114. Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies, concluded: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy

> World Wide Web content that exists on darknets: overlay networks that use the internet but require specific software, configurations, or authorizations to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

[37] *Hackers, Breaches, and the Value of Healthcare Data* (February 2, 2022), https://www.securelink.com/blog/healthcaredata-new-prize-hackers/ (last visited February 27, 2024).

[38] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (October 16, 2019), *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-darkweb-how-much-it-costs/ (last visited February 27, 2024).

[39] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (December 6, 2017), *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-yourpersonal-information-is- selling-for-on-the-dark-web/ (last visited Jan. 31, 2024).

medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[40]

115. In addition, criminals can purchase access to the entirety of a company's breached database on the dark web,[41] and would expect a sale price of $999.00 to $4,995.00.[42]

116. According to one Reuters report,[43] derived from an investigation including interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts:

- Medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information."
- According to investigating experts, fraudsters commonly use such medical data "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."
- A consumer's medical information is worth ten times more than the consumer's credit card number on the black market.

---

[40] *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottestitems- dark-web (last visited February 28, 2024).

[41] *See, e.g., In the Dark,* VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymousbrowsing/in-the- dark/ (last visited February 27, 2024)*; Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.16, 2019, *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-darkweb-how-much-it-costs/ (last visited February 27, 2024).

[42] *In the Dark,* VPNOverview (2019), *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited February 28, 2024).

[43] Caroline Humer and Jim Finkle, *Your medical record is worth more to hackers than your credit card*, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924/ (last visited February 28, 2024).

- Medical identity theft is often not immediately identified, giving cybercriminals years to "milk such credentials."

117. The Private Information compromised in a data breach within the healthcare industry, such as the Data Breach here, is significantly more valuable than the loss of, for example, credit card information in a large retailer data breach. Victims affected by retailer breaches could avoid much of the potential future harm by taking rather simple steps, including cancelling credit or debit cards and simply obtaining replacement cards. On the other hand, the information stolen in a healthcare industry data breach—such as sensitive medical information and Social Security numbers—is difficult, if not impossible, for the consumer to change.

118. Relatively basic information such as names, email addresses, and phone numbers, also has value to cybercriminals. In addition to practices such as "spamming" customers or launching "phishing" attacks using compromised names and emails, cybercriminals routinely combine this basic information with other compromised data to build a more complete profile of an individual. As reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails," it is often such consumer profiling that enables cybercriminals to successfully carry out additional phishing attacks or social engineering attacks.[44]

119. There is often a substantial time lag between when a harm occurs as the result of a breach and when the harm is discovered, as well as substantial lag time between the time when

[44] *See Dark Web Price Index: The Cost of Email Data*, available at https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited February 27, 2024).

Private Information is compromised and when it is used. According to the U.S. Government Accountability Office,[45] which performed a comprehensive analysis of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

120. In any event, once cybercriminals compromise Private Information, they often trade the information on the "cyber black market" for many years.

F. The Data Breach was a Foreseeable Risk

121. Healthcare entities in possession of Private Information—such as Defendants and the pharmacies and providers they serve—are particularly susceptible to cyberattacks. Therefore, as an entity subject to HIPAA and involved in the routine creation, collection, maintenance, and use of Private Information, Defendants were at a heightened risk of a cyberattack.

122. Cybercriminals and data thieves regularly target healthcare organizations because of the highly sensitive (and extremely valuable) information maintained by such entities, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and other private personal information of patients, customers, and employees.

123. In addition, "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data,

[45] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. Government Accountability Office (June 4, 2007), available at: https://www.gao.gov/products/gao-07-737 (last visited Feb. 27, 2024).

Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[46]

124. Identity theft of healthcare data is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," more than identity thefts involving banking and finance, the government, and the military or education.[47]

125. At all relevant times, Defendants' susceptibility to cyberattack was or reasonably should have been known and obvious to Defendants. The increased vulnerability of healthcare data to cyberattacks has been a known industry concern for over a decade. Defendants were on notice of numerous public announcements concerning data breaches affecting the healthcare industry, knew that the Private Information it created, collected, maintained, and used is highly coveted by and a frequent target of cybercriminals, and, upon information and belief, were notified directly by the government and other stakeholders of their susceptibility to attack.

126. At all relevant times, Defendants were or should have been aware of the significant number of individuals whose Private Information Defendants created, collected, and stored and, thus, the significant number of individuals who would be harmed by unauthorized access to its systems.

127. At all relevant times, Defendants were or should have been aware that the Private Information of Plaintiff and Class Members was an attractive target for malicious actors.

---

[46] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (October 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited February 27, 2024).

[47] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, February 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited February 28, 2023).

128. At all relevant times, Defendants knew or reasonably should have known of the importance of safeguarding Private Information and the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

129. Defendants' failure to safeguard Private Information is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data. Indeed, data breaches, such as the one experienced by Defendants have become so notorious that the FBI, U.S. Secret Service, and other authorities have issued warnings to potential targets so they are aware of, can prepare for and, hopefully, are able to ward off a potential attack.

130. As early as 2011, the FBI had issued warnings regarding the advancement in cybercriminals' abilities to remotely attack systems, particularly those in healthcare, and exploit the systems to obtain Private Information. This warning was not only a prediction of the general escalation of cybercrime, but also was a clear indication to entities such as Defendants of the impending risks associated with the storage and handling of sensitive healthcare data.[48]

131. As early as 2014, in response to a cyberattack on Community Health Systems Inc. and to enable entities within the healthcare industry to take necessary precautions to thwart such attacks, the FBI alerted the healthcare industry that it is an increasingly preferred target of cybercriminals. The FBI's "flash" alert stated,[49] in pertinent part:

> The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health

[48] Gordon M. Snow, *Statement before the House Financial Service Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cybersecurity-threats-to-the-financial-sector (last visited February 28, 2024).

[49] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (August 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2 4U20140820 (last visited February 28, 2024).

> Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

132. In an October 2, 2019 Public Service Announcement titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," the FBI reiterated to the healthcare industry and public that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[50]

133. The American Medical Association has also emphasized the significance of cybersecurity in healthcare, noting it as a technical concern and a vital aspect of patient safety, and highlighting that cyberattacks threaten patient access to care in addition to the privacy and security of patients' Private Information. According to research conducted by the American Medical Association, as of October 2019, 83% of physicians are part of practices that have been affected by cyberattacks.[51]

134. On March 10, 2021, the Tenable Security Response Team (SRT) published its analysis of data breaches between January 2020 and October 2020, concluding that the healthcare sector was "by far the most affected industry sector" and that "ransomware is the root cause in a majority of the healthcare breaches analyzed." According to its root cause analysis of 293 healthcare breaches known to have exposed records between January 2020 and February 2021, the

---

[50] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI Public Service Announcement, Alert Number I-100219-PSA (October 2, 2019), available at: https://www.ic3.gov/Media/Y2019/PSA191002 (last visited February 27, 2024).

[51] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, American Medical Association (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-downclinics-hospitals (last visited February 27, 2024).

Tenable SRT concluded that "ransomware was by far the most prominent root case of healthcare breaches, accounting for a whopping 54.95%."[52]

135. In addition to these industry-specific warnings, trends in cybercrime within the healthcare industry have demonstrated an alarming increase in the frequency and sophistication of attacks. These attacks include, without limitation, attacks on the following entities: American Medical Collection Agency (25 million patients in March 2019), University of Washington Medicine (974,000 patients in December 2018), Florida Orthopedic Institute (640,000 patients in July 2020), Wolverine Solutions Group (600,000 patients in September 2018), Oregon Department of Human Services (645,000 patients in March 2019), Elite Emergency Physicians (550,000 patients in June 2020), Magellan Health (365,000 patients in April 2020), and BJC Health System (286,876 patients in March 2020).

136. Indeed, in an article published by HHS on October 31, 2023, in an effort to bring awareness to Cybersecurity Awareness Month, HHS noted that "[r]ansomware and hacking are the primary cyber-threats in health care." According to HHS statistics, since 2019 there has been a 239% increase in large breaches reported to HHS' Office for Civil Rights and a 278% increase in ransomware attacks. Further, in the first ten months of 2023, more than 88 million individuals—one quarter of Americans—had their medical data exposed, a 60% increase from 2022.[53]

[52] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited February 27, 2024).

[53] HHS' Office for Civil Rights, *HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation* (October 31, 2023) https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attackinvestigation.html (last visited February 27, 2024).

137. In compiling and analyzing data breach statistics, for a period covering October 2009 through 2023, the HIPAA Journal reported:[54]

> Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the exposure or impermissible disclosure of 382,262,109 healthcare records. That equates to more than 1.2X the population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day.

138. The continual increase in data breaches within the healthcare industry underscored the necessity for Defendants to implement advanced security measures, such as robust encryption, regular security audits, and comprehensive employee training on cybersecurity.

139. In a Joint Cybersecurity Advisory issued on December 19, 2023, approximately two months prior to the Data Breach, the FBI and CISA encouraged critical infrastructure organizations such as Defendants to implement their various recommendations set forth in the advisory to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents. The FBI and CISA provided various step-by-step technical details associated with the ALPHV Blackcat criminal organization and its attack techniques, and advised organizations of "actions to take today," which included "prioritize remediation of known exploited vulnerabilities."[55]

140. Furthermore, days prior to the December 19 Joint Cybersecurity Advisory, on December 8, 2023, United Healthcare Services Inc. filed a notice of data breach with the Attorney

---

[54] The HIPAA Journal, *healthcare Data Breach Statistics*, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited February 27, 2024).

[55] *See* FBI and CISA Joint Cybersecurity Advisory (December 19, 2023), available at: joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat-12-19-2023.pdf (aha.org).

General of Montana after discovering that an unauthorized party accessed an e-mail account of one of its venders, Equality Health, leading to the theft of sensitive consumer information, including names, dates of birth, genders, addresses, Social Security numbers, Medicare and other membership identification numbers, Medicare plan information, and primary care provider information.

141. Based on the foregoing, it is beyond reasonable dispute that Defendants knew or should have known that their electronic records would be targeted by cybercriminals and had an obligation and duty to take all reasonable means to protect those records from attacks such as the Data Breach here.

142. Notwithstanding the common knowledge of, and the prevalence of public announcements and abundance of other publicly available resources with respect to, the imminent and serious threat of unauthorized access to Private Information within the healthcare industry; notwithstanding the data breach that had recently struck UnitedHealth; and despite its creation, collection, maintenance, and use of Private Information of millions of individuals, Defendants failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' Private Information. Had Defendants implemented adequate security measures, cybercriminals never could have accessed millions of individuals' files (as ALPHAV claims it apparently did) and the Data Breach would have been prevented or, at a minimum, of a much smaller scope.

G. The Data Breach Harmed and Will Continue to Harm the Class

143. Victims of data breaches are exposed to serious ramifications. Indeed, the reason why cybercriminals steal sensitive information is to monetize it.

144. Cybercriminals monetize stolen personal identification, health, and financial information by selling the spoils of their cyberattacks on the black market to identity thieves and other criminals to extort and harass victims or assume the victims' identities to engage in illegal financial transactions under the victims' names.

145. Victims of identity theft also routinely suffer embarrassment, harassment, or blackmail, in person or online, and/or experience financial losses (e.g., unauthorized account transactions and credit downgrades) resulting from, by way of example, fraudulently opened accounts or misuse of existing accounts.

146. The unencrypted Private Information of Plaintiff and Class members will end up (to the extent that it has not already ended up) for sale on the dark web, as that is the modus operandi of cybercriminals.

147. Given the type and scope of this targeted attack, the sophisticated cybercriminal activity, the volume of data compromised, and the sensitive type of Private Information involved in this Data Breach, entire batches of stolen information have undoubtedly been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes, including opening financial and other accounts in the consumer's name to make purchases or to launder money; filing of fraudulent tax returns; taking of loans or lines of credit; or filing of false unemployment or similar claims.

148. Unencrypted Private Information may also fall into the hands of other entities that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

149. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, the

reasonable person is expected to take steps and spend time to address the dangerous situation, learn the circumstances of the breach, and attempt to mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking such steps—including failure to constantly review accounts and credit reports—could expose the individual to greater financial harm.

150. Thus, due to the imminent risk of or completed identity theft, Plaintiff and Class Members must monitor their financial accounts for many years in an attempt to mitigate the risk of identity theft, and now face years of constant surveillance of their financial and personal records, other necessary monitoring, and loss of rights.

151. The retail cost of credit or identity theft monitoring is expected to be approximately $200 per year per Class Member. This is a reasonable and necessary cost to monitor and protect Plaintiff and Class Members from the risk of identity theft resulting from Defendants' Data Breach. This is a future cost for, at a minimum, five years. Plaintiff and Class Members would not be caused to bear this expense but for Defendants' failure to safeguard their Private Information.

152. Plaintiff and Class members have spent, and will continue to spend, time on a variety of prudent actions, such as changing passwords and re-securing their own computer systems.

153. Defendants' failure to properly safeguard Plaintiff's and Class Members' Private Information from cybercriminals has caused and will continue to cause substantial risk of future harm (such as identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off such highly sensitive information.

CLASS ALLEGATIONS

154. Plaintiff brings this class action individually on behalf of himself and on behalf of all members of the following classes and subclasses (collectively, the "Classes") of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23(a) and 23(b)(3) (as well as the requirements for certification of one or more issue classes under Rule 23(c)(4)).

155. Accordingly, Plaintiff seeks certification under Federal Rule of Civil Procedure 23 of the following Class and Subclasses:

- **Nationwide Class:** All individuals residing in the United States who participate in manufacturer savings card/"coupon" programs that utilize Defendants' systems and platforms and whose Private Information was exposed, accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.
- **Nationwide Class:** All individuals residing in the United States who participate in manufacturer savings card/"coupon" programs that utilize Defendants' systems and platforms and who were prevented from using such programs as a result of the Data Breach and the resulting disruption of processing of manufacturer savings card/"coupon" transactions.
- **Subclass:** All individuals residing in the United States who participate in manufacturer savings card/"coupon" programs that utilize Defendants' systems and platforms and whose prescription medications were not timely filled or refilled as a result of the Data Breach and the resulting disruption of processing of manufacturer savings card/"coupon" transactions.

- **Subclass:** All individuals residing in the United States who participate in manufacturer savings card/"coupon" programs that utilize Defendants' systems and platforms and who were forced to pay out of pocket for prescription medications as a result of the Data Breach and the resulting disruption of processing of manufacturer savings card/"coupon" transactions.

156. Excluded from the Classes are (1) Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, any entity in which Defendants have a controlling interest; (2) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (3) those persons who have suffered personal injuries as a result of the facts alleged herein (4) any and all federal, state, or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions; and (5) all judges presiding over this matter or assigned to hear any aspect of this litigation, along with judicial clerks and staff, and immediate family members.

157. Plaintiff reserves the right to modify or amend the foregoing Class and Subclasses definitions before the Court determines whether certification is appropriate.

158. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is readily ascertainable.

159. **Numerosity (Federal Rule of Civil Procedure 23(a)(1)):** A class action is the only available method for the fair and efficient adjudication of this controversy. The members of each Class are so numerous and geographically dispersed that individual joinder of all Class Members is neither practicable nor possible. Plaintiff is informed and believes and, on that basis, alleges that

the total number of Class Members is in the thousands—if not millions—of individuals. Membership in the Class will be determined by analysis of Defendants' records.

160. **Commonality (Federal Rule of Civil Procedure 23(a)(2) and (b)(3)):** Consistent with Rule 23(a)(2) and with Rule 23(b)(3)'s predominance requirement, Plaintiff and Class Members share a community of interest in that there are numerous common questions and issues of law and fact which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their Private Information;

b. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

c. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

d. Whether Defendants were negligent in maintaining, protecting, and securing Private Information;

e. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems;

f. Whether Defendants breached their duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the data breach was discovered;

h. Whether Defendants failed to take reasonable and prudent security measures;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants' security measures to protect its systems were reasonable in light of known legal requirements;

k. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

l. Whether Defendants violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

m. Whether Defendants violated federal statutes including, but not limited to, HIPAA and FTCA;

n. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

o. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

p. Which security procedures and notification procedures Defendants should be required to implement;

q. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

r. Whether Defendants' conduct, including its alleged failure to act, resulted in or was the proximate cause of the Data Breach and/or loss of Private Information of Plaintiff and Class Members;

s. Whether Defendants breached their duties to Plaintiff and Class Members with respect to timely and accurately processing manufacturer savings card/coupon programs for prescription medications;

t. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Private Information; and

u. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

161. In the alternative, Plaintiff seeks certification under Rule 23(c)(4) with respect to one or more of the above issues or such other issues as may be identified in the future.

162. **Typicality (Federal Rule of Civil Procedure 23(a)(3)):** Plaintiff's claims are typical of the claims of the Classes. Plaintiff's and Class Members' Private Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff sustained damages, akin to damages sustained by Class Members, arising out of and caused by Defendants' common course of conduct in violation of laws and standards, as alleged herein.

163. **Adequacy (Federal Rule of Civil Procedure 23(a)(4)):** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of each of the Classes because Plaintiff is a member of the Classes and is committed to pursuing this matter against Defendants to obtain relief for the Classes. Plaintiff is not subject to any individual defense unique from those conceivably applicable to other Class Members or the Classes in their entirety. Plaintiff anticipates no management difficulties in this litigation. Plaintiff has no conflicts of interest with the Classes. Plaintiff's Counsel is competent and experienced in litigating class actions, including extensive experience

in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

164. **Predominance and Superiority (Federal Rule of Civil Procedure 23(b)(3)):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation predominate over individual issues. The issues discussed above in regard to commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also burden and unreasonably strain the court system, and would result in undue delay. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

165. **Ascertainability:** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. Defendants have access to names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach.

166. **Injunctive and Declaratory Relief:** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and procedures hinges on Defendants' conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff. Unless a Class-wide injunction is issued, Defendants may continue failing to properly secure Class Members' Private Information, and Defendants may continue to act unlawfully, as set forth in this Complaint. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

CAUSES OF ACTION

COUNT ONE
Negligence
(*On Behalf of Plaintiff and the Classes*)

167. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

168. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of their businesses, which affect commerce.

169. The Private Information of Plaintiff and Class Members was entrusted to Defendants with the understanding that the information would be safeguarded.

170. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

171. It was reasonably foreseeable to Defendants that Plaintiff and the Class Members would suffer such harms in the event of a cyber-attack such as the Data Breach here.

172. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in Defendants' possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons .

173. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, consistent with industry standards and requirements, and to ensure that its computer systems, networks, and protocols, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information and allowed manufacturer savings card/"coupon" transactions to be timely and accurately processed.

174. Defendants also had a special relationship with Plaintiff and each of the Class Members. That special relationship arose because Defendants were entrusted with their confidential Private Information as a necessary part of healthcare-related services rendered by Defendants and because Defendants were entrusted with providing necessary means to process manufacturer savings card/"coupons" for prescription medications for Plaintiff and Class Members. That special relationship provides an additional basis on which Defendants owed a duty to Plaintiff and each of the Class Members to protect against unauthorized access to, theft of, and/or disclosure of their Private Information.

175. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that all Private Information in their possession or control was adequately secured and protected and that manufacturer savings card/"coupon" transactions to be timely and accurately processed.

176. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in their possession or control, including not sharing information with other entities who maintain sub-standard data security systems.

177. Defendants owed a duty to Plaintiff and Class Members to implement and maintain processes that would immediately detect a breach of their data security systems in a timely manner.

178. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

179. Defendants owed a duty to Plaintiff and Class Members to disclose in timely fashion if their computer systems and data security practices were inadequate in any way to safeguard individuals' Private Information, including from theft, because such an inadequacy would be a material fact in the decision to entrust Private Information to Defendants.

180. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' Private Information.

181. Defendants owed a duty to Plaintiff and Class Members to monitor user behavior and activity to identify possible threats to the confidentiality and integrity of Private Information.

182. Defendants owed a duty to Plaintiff and Class Members to promptly and adequately notify Plaintiff and Class Members of the Data Breach, but failed to do so.

183. Defendants owed a duty to Plaintiff and Class Members to design, manage, operate, and secure their platforms and systems in such a way as to ensure manufacturer savings card/"coupon" transactions for prescription medications would be timely and accurately processed.

184. Defendants had and continue to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within their possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and remains necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

185. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures.

186. Defendants knew or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on their systems, including the foreseeable risks that a cyberattack on Defendants' systems would result in delay and disruption for the timely and accurate processing of manufacturer savings card/"coupon" programs, depriving patients of necessary prescription medications that were unaffordable without such savings cards/"coupons."

187. Plaintiff and the Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession. Likewise, Plaintiff and the Class Members had no ability to ensure timely and accurate processing of the manufacturer savings card/"coupon" programs for which Defendants undertook to provide necessary systems and platforms.

188. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class Members as a result of the Data Breach.

189. Defendants' duties extended to protecting Plaintiff and the Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship.

190. Defendants failed to perform their duties by failing to reasonably and adequately secure their systems (and the Private Information of Plaintiff and the Class Members) against the Data Breach.

191. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiff and the Class Members, Plaintiff's and Class Members' Private Information would not have been exposed to the Data Breach and potentially compromised and the timely and accurate processing of manufacturer savings card/"coupon" programs run through Defendants' systems would not have been delayed and disrupted.

192. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class Members.

193. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class Members have suffered and will suffer injury, including delay and/or interruption of prescription medications, higher out of pocket costs for prescription medications, adverse health impacts, injury to their privacy and to the value of their Private Information, and other forms of injury and/or harm, including, but not limited to, emotional distress, loss of privacy, anxiety, annoyance, nuisance, and other economic and non-economic losses including nominal damages.

194. Plaintiff and Class Members are entitled to compensatory damages suffered as a result of the Data Breach.

195. On information and belief, Defendants' negligent conduct is ongoing, in that Plaintiff's and Class Members' Private Information is being maintained in an unsafe and insecure manner.

196. Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to: (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT TWO
Negligence Per Se
(*On Behalf of Plaintiff and the Classes*)

197. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

198. Defendants had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, the FTCA, and state data security and consumer protection statutes such as those outlined herein to protect Plaintiff's and Class Members' Private Information.

199. On information and belief, Defendants breached their duties, pursuant to HIPAA and FTCA, and other applicable standards by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

200. Defendants' violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, Section 5 of the FTCA, and similar state statutes constitutes negligence per se.

201. Plaintiff and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTCA were intended to protect.

202. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTCA were intended to guard against.

203. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

204. Plaintiff and Class Members were foreseeable victims of Defendants' violations of HIPAA, HITECH, and the FTCA, as well as state data security and consumer protection statutes. Defendants knew or should have known that their failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class Members.

205. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiff and the Class Members, Plaintiff's and Class Members' Private Information would not have been exposed to the Data Breach and potentially compromised and the timely and accurate processing of manufacturer savings card/"coupon" programs run through Defendants' systems would not have been delayed and disrupted.

206. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class Members.

207. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class Members have suffered and will suffer injury, including delay and/or interruption of prescription medications, higher out of pocket costs for prescription medications, adverse health impacts, injury to their privacy and to the value of their Private Information, and other forms of injury and/or

harm, including, but not limited to, emotional distress, loss of privacy, anxiety, annoyance, nuisance, and other economic and non-economic losses including nominal damages.

208. Plaintiff and Class Members are entitled to compensatory damages suffered as a result of the Data Breach.

209. On information and belief, Defendants' negligent conduct is ongoing, in that Plaintiff's and Class Members' Private Information is being maintained in an unsafe and insecure manner.

210. Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to: (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT THREE
Negligent Undertaking
(*On Behalf of Plaintiff and the Classes*)

211. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

212. By agreeing to process prescription claims, Defendants undertook to render services that benefitted Plaintiff and Class Members, including timely and accurate processing of manufacturer savings card/"coupon" programs for prescription medications.

213. In undertaking to provide such services, Defendants knew or should have known of the necessity to, *inter alia*, heed credible security warnings; maintain adequate patch management policies and procedures; detect alerts in regard to vulnerabilities affecting its systems; properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; properly use automated

tools to track which versions of software were running and whether updates were available; and implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

214. Only Defendants were in the position to ensure that their information systems, practices, and protocols were sufficient and consistent with industry standards and requirements.

215. Defendants failed to exercise reasonable care to perform these actions. Defendants failed to provide reasonable or adequate information systems and networks and failed to engage in appropriate cybersecurity practices to safeguard their services.

216. Defendants' failure to abide by their duties placed Plaintiffs and Class Members in a worse position than they would have been had Defendants not undertaken such duties because other, more secure means would have been used to process manufacturer savings card/"coupon" programs for prescription medications for Plaintiff and the Classes which would have avoided disruption of medications, delay, costs, and other injuries to Plaintiff and the Classes

217. Defendants' failure to abide by their duties was wrongful and negligent in light of the foreseeable risks and known threats.

218. Defendants knew or should have known that failure to take appropriate actions to secure its systems increased the risk of harm to Plaintiff and Class Members beyond the risk of harm that existed without the undertaking.

219. As a direct and proximate result of Defendants' negligent undertaking, Plaintiff and the Class Members have suffered and will suffer injury.

COUNT FOUR
Negligent Failure to Warn
(*On Behalf of Plaintiff and the Classes*)

220. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

221. Upon information and belief, Defendants were or should have been aware for a substantial period of time that their cybersecurity systems and networks were inadequate and prone to attack.

222. Upon information and belief, Defendants knew or should have known of its cybersecurity failures including, but not limited to, failing to heed credible security warnings; failing to maintain adequate patch management policies and procedures; failing to detect alerts in regard to vulnerabilities affecting its systems; failing to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failing to properly use automated tools to track which versions of software were running and whether updates were available; and failing to implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

223. Nevertheless, Defendants failed to warn Plaintiff and Class Members of the known cybersecurity vulnerabilities, failed to effectively remedy the cybersecurity flaws and problems in their systems and networks, failed to warn Plaintiff and Class Members of likely risks caused by Defendants' failure to remedy such cybersecurity flaws, and failed to provide prompt notice to Plaintiff and Class Members that the secure information systems had been breached by unauthorized persons during the Cyberattack.

224. As a direct and proximate result of Defendants' negligent failure to warn, Plaintiff and the Class Members have suffered and will suffer injury.

COUNT FIVE
Unjust Enrichment
(*On Behalf of Plaintiff and the Classes*)

225. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

226. This count is pleaded in the alternative to the breach of implied contract claim above.

227. Plaintiff and Class Members conferred a monetary benefit on Defendants in connection with obtaining healthcare services (including prescriptions), specifically providing Defendants directly or indirectly with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants services or benefits that were the subject of the transaction, and should have had their Private Information protected with adequate data security.

228. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiff's and Class members' retained data and the use of Plaintiff's and Class Members' Private Information for business purposes.

229. Defendants failed to take action and update their systems to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

230. Defendants acquired Plaintiff's and Class Members' Private Information through inequitable record retention as they failed to disclose the inadequate vendor vetting and data security practices previously alleged.

231. Had Plaintiff and Class Members known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure

their Private Information, or vendors that house their Private Information, they would not have entrusted their Private Information to Defendants.

232. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

233. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class Members have suffered and will suffer injury.

234. Plaintiff and Class Members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants as a result of their wrongful conduct, as well as the return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

235. Plaintiff and Class Members may not have an adequate remedy at law against Defendants and, accordingly, plead this count in addition or as an alternative to the other counts plead herein.

COUNT SIX
Declaratory Judgment
(*On Behalf of Plaintiff and the Classes*)

236. Plaintiff restates, re-alleges, and incorporates by reference each and every allegation of the preceding paragraphs of this Complaint as though fully set forth herein.

237. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

238. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Defendants' data security measures and third-party vendor vetting remain inadequate. In addition, Plaintiff continues to suffer injuries as result of the exposure of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

239. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure Plaintiff's and Class Members' Private Information, select vendors who handle Private Information that will adequately safeguard that information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTCA, HIPAA, and various state statutes;

b. Defendants also owe a legal duty to adequately safeguard against cyberattacks that foreseeably delay and disrupt processing of manufacturer savings card/"coupon" programs and, in turn, foreseeably interrupt, delay, or deprive patients like Plaintiff and Class Members of otherwise unaffordable prescription medication and/or force such patients to pay out of pocket for such medications; and

c. Defendants breached and/or continue to breach this legal duty by failing to employ reasonable measures to secure Private Information in their possession and/or the systems and platforms they use to process manufacturer savings card/"coupon" programs.

240. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment awarding Plaintiff and the Classes equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

A. enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein pertaining to the misuse, failure to protect, and/or disclosure of Plaintiff's and Class Members' Private Information and/or failure to protect the systems and platforms they use to process manufacturer savings card/"coupon" programs;

B. requiring Defendants to implement appropriate security protocols designed to protect the confidentiality and integrity of Private Information, including through:

i. utilization of appropriate methods, procedures, and policies with respect to collection, storage, and use of Private Information and/or processing of manufacturer savings card/"coupon" programs;

ii. encryption of all data collected through the course of business in accordance with applicable regulations, industry standards, and federal, state, and local laws;

iii. monitoring of ingress and egress of all network traffic;

iv. engaging independent third-party auditors and internal personnel to run automated security monitoring, simulated attached, penetration tests, and audits on Defendants' systems;

v. segmenting of data by creation of appropriate firewalls and access controls; and

vi. establishing an appropriate and/or supplementing their existing information security training programs;

C. compelling Defendants to issue prompt, complete, specific, and accurate disclosures to Plaintiff and Class Members, with respect to all Private Information compromised as the result of the Data Breach;

D. requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

E. compelling Defendants to facilitate, maintain, and/or pay for credit monitoring services for Plaintiff and the Classes, for a period not less than five years;

F. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

G. appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis, for a period of ten years, to evaluate Defendants' compliance with the terms of the Court's final judgments, to provide such report to the Court and counsel for the Class, and to report any deficiencies with compliance with the Court's judgment.

241. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the

resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

242. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

243. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at or by Defendants, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the proposed Class and Subclasses, respectfully request that the Court enter judgment in Plaintiff's favor and against Defendants as follows:

A. Declaring, adjudging, and decreeing that this action is a proper class action, and certifying each of the proposed Classes and/or any appropriate Subclasses pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), and/or (b)(3), including designating Plaintiff as Class representative and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class and Subclasses appropriate monetary relief, including actual damages; statutory damages; consequential damages; punitive damages; exemplary damages; nominal damages; restitution; and disgorgement of all earnings, interest,

profits, compensation, and benefits received as a result of their unlawful acts, omissions, and practices;

C. Awarding Plaintiff and the Class and Subclasses equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

1. enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein pertaining to the misuse, failure to protect, and/or disclosure of Plaintiff's and Class Members' Private Information and/or failure to protect the systems and platforms they use to process manufacturer savings card/"coupon" programs;
2. requiring Defendants to implement appropriate security protocols designed to protect the confidentiality and integrity of Private Information, including through:
    a. utilization of appropriate methods, procedures, and policies with respect to collection, storage, and use of Private Information and the processing of manufacturer savings card/"coupon" programs;
    b. encryption of all data collected through the course of business in accordance with applicable regulations, industry standards, and federal, state, and local laws;
    c. monitoring of ingress and egress of all network traffic;
    d. engaging independent third-party auditors and internal personnel to run automated security monitoring, simulated attached, penetration tests, and audits on Defendants' systems;

e. segmenting of data by creation of appropriate firewalls and access controls; and

f. establishing an appropriate and/or supplementing its existing information security training program;

3. compelling Defendants to issue prompt, complete, specific, and accurate disclosures to Plaintiff and Class Members, with respect to the Private Information compromised as the result of the Data Breach;

4. requiring Defendants to meaningfully educate Plaintiff and all Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

5. compelling Defendants to facilitate, maintain, and/or pay for credit monitoring services for Plaintiff and the Classes, for a period not less than five years;

6. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

7. appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis, for a period of ten years, to evaluate Defendants' compliance with the terms of the Court's final judgments, to provide such report to the Court and counsel for the Class, and to report any deficiencies with compliance with the Court's judgment.

D. Compelling Defendants to pay the costs associated with notification of Class Members about the judgment and administration of claims;

E. Awarding Plaintiff and the Class and Subclasses pre-judgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class and Subclasses reasonable attorneys' fees, costs, and expenses; and

G. Awarding Plaintiff and the Class and Subclasses such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class and/or Subclass(es), hereby demands a trial by jury of all issues in this Complaint so triable.

Dated: March 25, 2024

Respectfully submitted,

John T. Spragens (TN No. 31445)
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
Telephone: (615) 983-8900
Facsimile: (615) 682-8533
john@spragenslaw.com

Jennifer R. Scullion*
Christopher L. Ayers*
Justin M. Smigelsky*
Nigel Halliday**
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
Telephone: (973) 639-9100
Facsimile: (973) 639-9393
jscullion@seegerweiss.com

cayers@seegerweiss.com
jsmigelsky@seegerweiss.com
nhalliday@seegerweiss.com

Attorneys for Plaintiff and the Proposed Classes
**Pro Hac Vice* forthcoming
** Tennessee Bar. Application for Admission to Middle District of Tennessee forthcoming